External Audit Report on Information Technology: Progress Report
Report by John Blair, Director, Corporate Resources

1. Introduction

This report presents progress with the recommendations made by Grant Thornton, External Audit, at the September 2012 Audit Committee. The committee requested a progress report before the end of the calendar year.

2. Background

Grant Thornton, the Council's External Auditors, presented their interim report to the Audit Committee on 18 September 2012 and in the report were four recommendations relating to Corporate IT Resilience. These were as follows:-

- that the Council should not have its primary computer server room (ground floor, Midlothian House) close to its secondary server room (first floor, Fairfield House) and should identify accommodation away from Dalkeith to reduce the risk of both servers being destroyed at the same time;
- IT services have produced a number of business continuity plans for their IT applications but should have a systematic testing strategy;
- The Midlothian House server room has an electric back-up generator but the Fairfield House one does not; this should be rectified; and
- The fire extinguisher at the Fairfield House server room had not been serviced for some time and this should be regulated

All four recommendations have been discussed in two forums:-

1. at the Council's Contingency Planning Group meeting on 14 November 2012; and
2. at meetings between IT Services and Internal Audit since the last Audit Committee.

Details of these discussions inform this report and set out the position.

3. Assessment of Options

<u>Recommendation 1 and locating secondary server room elsewhere</u>

The IT Service response to this recommendation was to include this issue within the Effective Working in Midlothian (EWiM) project and an indicative date for a solution targeted as 31 March 2017. The Audit Committee on 18 September resolved that IT Services should consider other options earlier and report back.

Previously IT Services has considered the risk of having two computer rooms close to each other and concluded that the risk would have to be accepted mainly because of cost. However, this risk has been recently re-assessed and the conclusions are:-

- Locating the secondary server room in another Council building such as Dundas Buildings or Penicuik Town Hall would be very expensive and an

initial estimate would be in the region of £250,000. There would also be significant resource and time requirements;

- Locating the secondary server room in the PPP Campus in Dalkeith is also an expensive option, as is an arrangement with a Computer Bureau in terms of a 'warm-start' solution;
- In carrying the temporary risk, until the EWiM solution is delivered, it is worthwhile considering compensatory controls in relation to worst case scenarios and less dramatic threats; and
- In relation to the previous bullet point, these scenarios and threats have recently been discussed during a six-monthly audit assessment. A copy of this assessment is attached and it covers not only the server room issues but other IT risks.

Members will see from the attached assessment that there are several mitigating controls in place to make the interim period acceptable in being able to balance and accept an element of risk. Members should also be aware that Internal Audit is liaising with IT Services on a regular basis to confirm that internal controls measures are robust.

Recommendation 2 and Testing of IT Applications Recovery

IT Services have discussed this with the Contingency Planning Officer and an exercise is currently underway to:-

- Confirm the staffing establishment, job titles and roles and responsibilities and accommodation within the three divisions;
- Establish the importance of each service in terms of a community incident or an internal incident. With the former it could be a major incident of such proportion that Council services and citizens would be seriously affected. With the latter it could be a scenario that a Council building is affected by fire or water ingress;
- Understand the importance of critical computer systems in relation to the above that may have to be recovered in a short space of time; and
- Ensure that all business recovery plans are tested and exercised on a regular and incremental basis.

This 'Business Impact Analysis' (BIA) is an essential requirement under the Civil Contingencies legislation. The BIA will help in the updating of key building Recovery Plans e.g. if Midlothian House is impacted by fire, the Recovery Plan will detail where the staffing could be moved to and the critical IT systems they would need in their new premises.

This process (BIA) across all three divisions will be completed by Christmas and will bring further certainty to business recovery. Meantime, IT Services continue to incrementally test critical IT systems in terms of recovery and this will continue this after New Year under the umbrella of a refreshed and updated BIA and IT Recovery Plan.

Recommendation 3 and Back-Up Generator for Fairfield House Server Room

An estimate indicates that procuring a generator for Fairfield House would cost in excess of £30,000 and the view is that it may be appropriate to wait until the EWiM project is in place and have new server rooms fully supported by back-up generators.

Recommendation 4 and Fire Extinguisher in Fairfield House Server Room

Issue has been resolved.

4. Resource Implications

4.1 Resource

The cost of moving the second computer room to another location like the Schools Campus or another Council building appears prohibitive at this stage. The costs of the extra connection to the standby generator are outlined above.

7.2 Risk

This is a situation of balancing risk, likelihood and impact and the attached assessment outlines the current controls and the control of risk.

7.3 Policy

Strategy – the EWiM project, if progressed, will rationalise the Council's property needs and a strengthening of IT Resilience is programmed into the project.

Consultation – the Head of Customer Services, Head of Finance and Human Resources, IT Infrastructure Manager, Internal Audit and Head of Property and Facilities Management have all been consulted in the preparation of this report.

Equalities – There are no equalities issues in this report.

Sustainability – This report suggests a way forward in having assurance over the computer facilities of the Council.

4. Recommendations

The Audit Committee is invited to:-

1. Scrutinise this report and the attached assessment; and
2. Note that Internal Audit is carrying out ongoing checks on the internal controls highlighted in the assessment.

3 December 2012

Report Authors:

Steve Currer, IT Infrastructure Manager
Tel: 0131-271-3030
E-Mail: Steve.currer@midlothian.gov.uk
and
Gerald Tait, Risk and Audit Manager
Tel: 0131-271-3284
E-Mail: Gerald.tait@midlothian.gov.uk

Appendix

Corporate IT Resilience: Internal Control Assessment
November 2012

Introduction

An internal control assessment into Corporate IT Resilience was presented to the Audit Committee in February 2011 and has been monitored since by management and been appended to a registered risk within the Customer Services operational risk register.

The External Auditors, Grant Thornton, reviewed IT resilience during this summer 2012 and presented their report to the Audit Committee on 18 September 2012. The Audit Committee has requested a progress report by Christmas 2012 in respect of certain IT Resilience matters.

The Internal Audit team has an audit assignment on Corporate IT Resilience planned before the end of this financial year 2012/13.

After having discussed these matters with the IT Infrastructure Manager, it seemed worthwhile to wrap all three reviews above into a fresh internal control assessment (below).

Internal Control Assessment – subject to ongoing review

Topic	Established Controls
Contracts with Hardware & Software Suppliers	1. Main applications – contractual agreements set up for licensing, support and service levels; 2. Financial checks by the procurement team on suppliers at tender stage; 3. Annual financial checks on main suppliers; 4. Monitoring of contractual performance by services using the applications; 5. Should a supplier become insolvent, back-up insurance is not considered appropriate and reliance would more than likely be placed on identifying another supplier who would purchase the software rights. Generally system applications use the same code etc. There has been no real history of software suppliers becoming insolvent; however, recently HFX, the supplier of the staff flexitime system, became insolvent and another firm took up the contract forthwith 6. Council can normally still use the software, should a supplier become insolvent. However, this can depend on each contract in terms of copyright, intellectual and perpetuity rights.
Changes to Software – security and software updates	1. Controlled patch and change control 2. Corporate IT can normally change computer systems and within this service, only Infrastructure staffing can perform this function. However, IT Development Services occasionally require permission from Infrastructure to make updates, however the numbers of personnel involved is limited. 3. Adoption of ITIL Change Management procedures, a recognised method of computer change management. 4. ITIL is however only used for changes to applications e.g. Academy, Frameworki 5. For matters like Microsoft security patches, they would be implemented outside ITIL. If there was a significant update of Microsoft, then a 'project' would be set up outside ITIL. 6. ITIL Change Management is led by a Senior IT Support Analyst 7. ITIL adopts a 'Request for Change' model (RFC) 8. This is within the IT Help Desk software 9. All changes are serially numbered 10. All requests for changes have to be registered with the IT help desk, RFC 11. Members of the Infrastructure team normally have the opportunity to comment on each change and record their comments within the software; therefore there is separation of duties and obstacles placed in the way of wrong-doing or error. Other IT services can be involved. If appropriate, the Information Security Officer is one of the officers making comments on the proposed change 12. Network activity logs are not monitored as this is a significant task and there

Topic	Established Controls
	are other priorities for resource. However, the application of a suitable tool to simplify this process is currently being investigated. 13. Computer applications should have developed exception reporting to highlight any unusual transactions. Within main Financial Systems this is a regular focus of attention for Internal Audit. 14. Normally every computer user has a unique ID and log-in.
Business Continuity Management (BCM)	Two computer rooms within 100 metres of each other (Midlothian and Fairfield Houses), albeit separated by a car park and the two premises are separate buildings:- <u>Worst Case Scenarios</u> Both buildings simultaneously destroyed, or partly destroyed, leaving the Council without IT systems e.g. Fire, Severe Water Ingress, Plane Crash, Lengthy Power Disruption; Malicious Damage caused by an employee or an intruder, situation like a severe gas leak in Dalkeith which would not allow IT staff near the buildings. All these scenarios have a low or very low likelihood but with a major impact on the Council and its services. Therefore, if the focus is on the EWiM project to produce a solution in the medium term, in the interim period the Council's officers and elected members are required to consider the existing risk control measures and likelihood of both buildings being affected simultaneously by the above threats. For example, is there a likelihood that both buildings could be subject to a fire and therefore a robust focus should be placed on the prevention and damage limitation measures? Here are the current internal controls:- 1. Full data and system back up every Friday 2. This picks up all data and any changes to the system in the previous week 3. Incremental back up 4 times a week – Monday to Thursday. Back ups are usually conducted overnight but can run into the next day. These accommodate updated and new data and any incremental changes to the system. 4. Extensive server capacity exists in Corporate IT, with Midlothian House making up about 60% of the corporate IT capacity. Fairfield House makes up a large part of the other server capacity percentage with buildings like Jarnac Court and Dundas Buildings making up the balance; 5. In terms of the capacity, there are 3 virtual servers in Midlothian House computer room and 3 in Fairfield House computer room. 6. Virtual servers aid resilience and efficiency in that within each server 'sub-servers' can be created, as many as capacity allows. However, use of each virtual server normally doesn't exceed 50% capacity, allowing spare room. 7. Therefore, test data can be held on a virtual server in Fairfield House with live data held on another virtual server in Midlothian House. Also two sets of live data can be held on separate virtual servers. 8. In an emergency, this would allow faster recovery of a critical application 9. If a new server has to be built it would require the installation of the operating system e.g. Microsoft, then the system application and then the latest data. 10. Normally application system discs are held within IT or can be obtained from the supplier 11. Virtual server use means that problems can be fixed during the day because servers can be shut down, knowing the data and system is held elsewhere 12. Virtual server use makes up about 50% of server activity 13. There are ordinary servers in Dundas Buildings, Jarnac Court, Loanhead Social Work Centre, Newbyres Village and Penicuik Town Hall 14. Each back up is 'instructed' through software called Commvault Galaxy. 15. All back ups are stored on the Primary Storage within the Midlothian House computer room, on ordinary servers 16. Once Primary back up is concluded, the software 'instructs' a Secondary Storage, into another ordinary server in the computer room in Jarnac Court. Jarnac Court is chosen as the secondary storage because it is further away

Topic	Established Controls
	from Midlothian House than Fairfield House, although it is also in Dalkeith. 17. Once the Secondary Storage is concluded, a tape is produced in Midlothian House and taken to Fairfield House to be stored in a locked safe. This form of back-up occurs every week. 18. By having various servers, test and live data can be held on these, thus spreading the risk. Test and live data need not be held on the same servers and these same servers need not be in the same building 19. Some systems can be hosted on separate servers, even as many as three for the application, live data and test data. This can spread the risk and assist recovery 20. If Midlothian House computer room was 'down', the computer room of Fairfield House would be used for the recovery and vice-versa 21. If the primary server in Midlothian House is 'down' then the main back-up server is not available and around 60% of the Council's server capacity would be unavailable. Therefore, the capacity in Fairfield House would have to be relied upon and be developed. Critical systems would have to be recovered first and an indication is that this may take up to 5 days. 22. The closure of Jarnac Court is likely to be part of the EWiM project rationalisation and therefore the secondary back up arrangement will have to be reviewed sometime in the future. 23. De Duplication software is used in back up and this sorts and analyses data as it is backed up, thus aiding back up efficiency. The software recognises duplicate, or more, files and only backs-up one version, thus reducing the space required for back-up. 24. There is the advantage that Microsoft- based files could be recovered quicker than applications. This is because they are simpler to restore. All services use these files 25. In terms of other 'lost' work, like income imports of customer income from banks, imports would be able to be repeated.
Protection of Data against Loss, Corruption or System Failure	1. IT Recovery Plan tested and exercised on a periodic basis 2. Computers systems listed as to their recovery priority 3. System-disks are stored in safes in both Midlothian and Fairfield Houses but are also held by the software suppliers 4. Refreshment and update of Business Recovery Plans (BIA) underway (November/December 2012).
Protection of the computer rooms	1. Each of the computer rooms is locked and swipe cards allocated to a limited number of IT personnel and the M&E Engineer. However, the intruder would have to pass through several locked doors before entering the computer room 2. The computer rooms have cameras and any out-of-hours intruders would be identified 3. There are two air conditioning systems in both the Midlothian House and Fairfield House computer rooms. These interact and if one failed, the other would produce extra capacity within the room. 4. Water tank control 5. Fire risk assessments and drills 6. Fire alarm systems 7. Fire extinguishers, properly serviced 8. Out-of-hours alert to East Lothian Contact Centre > Midlothian Clerk of Works > M&E Engineer > IT Infrastructure Manager
Power failure	1. Back-up generator for Midlothian House computer room, located in the Midlothian House car park 2. No back-up generators for other buildings, although back-up is being explored for Fairfield House 3. Back-up generator tested regularly; arranged by M&E Engineer 4. UPS (Uninterrupted Power Supply) systems in all computer rooms. Can respond for 20 minutes while back-up generator activates 5. UPS is linked to various servers
Insurance transfer of risk	1. Computer equipment covered for £2.5m with insurance excess of £500 2. Reinstatement of data cover of £100,000 with a £500 excess 3. Increased cost of working £50,000, indemnity period 12 months with an excess of £500 4. Insurance Tender documents indicate that virus and terrorism damage

Topic	Established Controls
	would be covered
Access to the system i.e. that all corporate IT users have properly controlled access.	1. IT staff allowed access are known and controlled 2. Authorised signatories database allows a service manager to authorise new staffing requiring access to networks and applications 3. HR and service managers notify IT of leavers. 4. Segregation of duties within corporate IT is activated through three separate teams: Infrastructure, Business Services and Development 5. Relevant IT Infrastructure staff have access to applications and data 6. IT Business Services staffing have no access, or very rare access, to live systems. Occasionally access is given but this has to be properly signed-off 7. IT Development staffing only have access to databases. 8. All senior officers in IT Infrastructure Services responsible for admin level access i.e. super-user are subject to ITIL Change Management 9. Unique log-ins apply to IT Infrastructure work 10. Password complexity follows UK government guidance 11. 8 characters in length and comprises a mix of alpha, numeric and upper and lower case characters 12. All leavers automatically deleted from networks and applications after 90 days of inactivity
Risk Management	1. Information Security Officer maintains a risk register in pursuit of ISO principles 2. Customer Services Risk Register covers IT Resilience 3. Risk Register reviewed each quarter with any high risks elevated to senior agendas.
External Hacking, External Issues etc	1. Anti-virus software installed on every computer 2. Software checks for viruses every 60 minutes, 24/7 3. If files are opened, they are automatically scanned for viruses 4. Defensive, in-depth approach with multiple virus products and checking takes place over e-mails 5. Firewall 6. Software patching adopted as a security measure as well as a system update 7. E-mail and web filtering, e-mail scanned for viruses, spam and phishing before reaching the Council's network by a company called Websense 8. E-mail then passes to the SMTP gateway where different technology filters the e-mails for problems 9. Additional checks also remove unwanted file types such as code, executables and inappropriate content. E-mail is finally passed to the e-mail servers and scanned for viruses again 10. All access to the internet (web) is filtered by Websense software that blocks access to inappropriate websites and also prevents the downloading of unwanted content such as movie and music files, malicious applications and code. 11. Penetration testing – external consultants. Carried out on an ad-hoc basis by government-approved testers 12. Any new web-facing application or service is also subjected to testing before go-live. A report is produced by external consultants and any recommendations are acted upon by the Information Security Officer 13. Software suppliers wanting access to our computer systems require to follow ITIL (RFC) and sign a Non-Disclosure Agreement 14. GSX security requirements raise baseline security. This is the government-sponsored security over networks and the Council has recently been the subject of a government inspection 15. Laptop encryption and occasional controlled recall 16. Memory sticks risk assessed and encrypted on issue 17. Personal memory sticks won't work on Council computers 18. Guidance for officers sharing/transferring personal and sensitive data 19. Information Management Group and Action Plan 20. Data Protection Policy 21. Data Custodian based in corporate IT 22. Reporting to the centre of IT Incidents, investigated and logged/reported 23. Clear-desk policy 24. Main buildings have secure access and a Building Security Policy